



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 430
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-------------------------|-------------|----------------------|---------------------|------------------|
| 09/895,498 | 06/29/2001 | James S. Magdych | NAIIP012/01.132.01 | 8154 |
| 28875 | 7590 | 04/21/2006 | EXAMINER | |
| Zilka-Kotab, PC | | | SHIFERAW, ELEN I A | |
| P.O. BOX 721120 | | | ART UNIT | PAPER NUMBER |
| SAN JOSE, CA 95172-1120 | | | 2136 | |

DATE MAILED: 04/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/895,498

Applicant(s)

MAGDYCH ET AL.

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 January 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4-20 and 22-39 is/are pending in the application.
- 4a) Of the above claim(s) 3 and 21 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,4-9, 15-20, 22-27, and 33-39 is/are rejected.
- 7) ☐ Claim(s) 10-14 and 28-32 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Applicant's arguments and amendments with respect to amended claims 1, 18, and 36-38, previously canceled claims 3 and 21, and presently pending claims 1-2, 4-20, and 22-39 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-2, 4-9, 19-20, 22-27, and 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bunker, V et al. (herein after Bunker) Pub. No.: US 2003/0028803 A1 in view of Berstis et al. (herein after Berstis) USPN 6,549,972 B1.

Regarding claims 1, 18 and 36, Bunker discloses a method/program product/system for

detecting modifications to risk assessment scanning caused by an intermediate device, comprising:

- (a) initiating a risk assessment scan at and on a target from a remote source utilizing a network (0015 and 0093; *remote source/Command Engine initiating assessment test remotely on the target 1002*);
- (b) determining whether the risk assessment scan at and on the target involves an intermediate

Art Unit: 2136

- device coupled between the target and the remote source (0129 and 0095-0101; *risk assessment ... SSH, NMAP ... determining/detecting IP spoofer/unauthorized intermediate host*);
- (c) receiving results of the risk assessment scan from the target utilizing the network (0083; *Command Engine receiving risk assessment test results from target computer remotely*); and
- (d) notifying an administrator if it is determined that the risk assessment scan at and on the target involves the intermediate device (0126, 0115; *PortSentry Tool... alerts administrators to unsolicited probes ... spoofing, malicious attacks, denial of attack made by intermediate host during target risk assessment*), wherein **additional operations** are carried out to improve a risk assessment at and on the target in view of the presence of the intermediate device coupled between the target and the remote source (0095, 0126, 0163, and 0171; *Command Engine reacting... for test results received from target computers...performing new scan 516... CGI-scanner, whisker, cgichk, mesalla, port scanner, nmap, udpscan netcat... ping traceroute, slayer ICMP, ..., sending warning alert... for security measures and/or to improve risk assessment scan*); wherein a **plurality of procedures** are utilized to determine whether the risk assessment scan involves the intermediate device (0095-0101 and 0129; *multiple procedures are performed to determine IP spoofer/unauthorized intermediate host between the target node and Command Engine device... port scanner, whisker scanner...*).

Banker discloses remotely initiating risk assessment scans and performing risk assessment scans at and on the target and detecting *malicious attacker node or spoofer intermediate host pretending to be the existing router by modifying IP address of the existing router* for the messages exchanged between the initiator device/Command Engine and target device (0129 and 0095-0101). Banker fails to explicitly describe the involvement of the intermediate device as Applicant repeatedly argued.

However Berstis teaches detecting a snooper intermediate device that modifies and/or counterfeits messages by intercepting the communications exchanged between communication device and gateway (col. 5 lines 25-39).

Therefore it would have been obvious to one ordinary skill in the art at the time of the invention was made to modify the teachings of detecting the involvement of intermediate device that intercepts the messages exchanges between two nodes within the system of Bunker because it would detect and identify the router if the router modifies the risk assessment result messages exchanged between the remote initiator and target device. One would have been motivated to do so because it would allow providing an accurate risk assessment result without the router modifying the proper assessment results sent from the target node to remote initiator.

Regarding claims 37 and 38, Bunker discloses a method/program product for detecting modifications to risk assessment scanning caused by a proxy server, comprising:

- (a) initiating a risk assessment scan at and on a target, from a remote source utilizing a network (0015 and 0093; *remote source/Command Engine initiating assessment test remotely on the target 1002*);
- (b) executing a plurality of procedures to determine whether the risk assessment scan at and on the target involves a proxy server coupled between the target and the remote source (0095-0101 and 0129; *multiple procedures are performed to determine IP spoofer/unauthorized intermediate host between the target node and Command Engine device... port scanner, whisker scanner...*);
- (c) said procedures utilizing a plurality of parameters selected from the group consisting of an ip_ttl flag, a tcp-win flag, a via tag, and a host header value (*Examiner takes an official notice for limitation (c) as Applicant admits ip_ttl flag, and tcp_win flag as a well known (see, Applicant's Admitted Prior Art/AAPA/disclosure page 9 par. 4-page 10 par. 2). It would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of AAPA within the system of Bunker because it would allow to determine unauthorized (intermediate) device by comparing the values of the flags. Data is sent to different nodes and tag values are compared. If the tag values are different identify the new node*);
- (d) receiving results of the risk assessment scan from the target utilizing the network (0083; *Command Engine receiving risk assessment test results from target computer remotely*);
- (e) flagging the results of the risk assessment scan if at least one of the procedures indicates that the risk assessment scan involves a proxy server coupled between the target and the remote source (0126 and 0100); and

Art Unit: 2136

- (f) notifying an administrator if the results of the risk assessment scan at and on the target are flagged (0126, 0115; *PortSentry Tool... alerts administrators to unsolicited probes ... spoofing, malicious attacks, denial of attack made by intermediate host during target risk Assessment*);
- wherein additional operations are carried out to improve a risk assessment at and on the target in view of the presence of the proxy server coupled between the target and the remote source (0095, 0126, 0029, 0163, and 0171; *Command Engine reacting... for test results received from target computers...performing new scan 516... CGI-scanner, whisker, cgichk, mesalla, port scanner, nmap, udpscan netcat... ping traceroute, slayer ICMP, ..., sending warning alert upon detection of ... a spoofer node pretending to be the existing router by modifying IP address of the existing router ... for more security measures and/or to improve risk assessment scan*).

Banker discloses remotely initiating risk assessment scans and performing risk assessment scans at and on the target and detecting *malicious attacker node or spoofer intermediate host pretending to be the existing router by modifying IP address of the existing router* for the messages exchanged between the initiator device/Command Engine and target device (0129 and 0095-0101). Banker fails to explicitly describe the involvement of the intermediate device as Applicant repeatedly argued.

However Berstis teaches detecting a snoop intermediate device that modifies and/or counterfeits messages by intercepting the communications exchanged between communication device and gateway (col. 5 lines 25-39).

Therefore it would have been obvious to one ordinary skill in the art at the time of the invention was made to modify the teachings of detecting the involvement of intermediate device that intercepts the messages exchanges between two nodes within the system of Bunker because it would detect and identify the router if the router modifies the risk assessment result messages exchanged between the remote initiator and target device. One would have been motivated to do so because it would allow providing an accurate risk assessment result without the router modifying the proper assessment results sent from the target node to remote initiator.

Regarding claims 2, 19-20, and 39, Bunker and Berstis further discloses the method/program product, wherein the intermediate device includes a router/proxy server (Bunker 0129, and Berstis col. 5 lines 25-39).

Regarding claims 4, and 22, Bunker further discloses the method/program product, wherein at least one of the procedures includes determining a port list associated with the risk assessment (0095-0102; *nmap*, *udpscan*, *netcat port scanners*).

Regarding claims 5, and 23, Bunker further discloses the method/program product, wherein the at least one of the procedures further includes determining whether a value of a flag is different for communication attempts using at least two ports on the port list (0098-0103 and 0126).

Art Unit: 2136

Regarding claims 6, and 24, Bunker and Berstis disclose all the subject matter as disclosed above. AAPA discloses the method/program product, wherein the flag includes an ip ttl flag (Examiner takes official notice as Applicant admits ip_ttl flag is well known (*see, Applicant's Admitted Prior Art/AAPA/disclosure page 9 par. 4-page 10 par. 2*)). The rational for combining are the same as claim 37 above.

Regarding claims 7, and 25, Bunker and Berstis disclose all the subject matter as disclosed above. AAPA discloses further discloses the method/program product, wherein the flag includes a tcp_win flag (Examiner takes official notice as Applicant admits tcp_win flag is well known (*see, Applicant's Admitted Prior Art/AAPA/disclosure page 9 par. 4-page 10 par. 2*)). The rational for combining are the same as claim 37 above.

Regarding claims 8, and 26, Bunker further discloses the method/program product, wherein the communications include connection attempts between the remote source and the target utilizing the network (fig. 9).

Regarding claims 9, and 27, Bunker further discloses the method/program product, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the value of the flag is different for the communication attempts using the at least two ports on the port list (0098-0103 and 0129).

4. Claims 15-17 and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bunker, V et al. (herein after Bunker) Pub. No.: US 2003/0028803 A1 in view of Berstis et al. (herein after Berstis) USPN 6,549,972 B1, and further in view of Miles et al. (Miles, Patent No.: US 6,886,044 B1).

As per claims 15, and 33, Bunker and Berstis disclose all the subject matter as described above. Bunker and Berstis do not disclose a method/program, wherein at least one of the procedures includes transmitting a request without specifying a host header value.

However Miles discloses displaying an error message when unidentified/unknown header value is received (col. 23 lines 66-col. 24 lines 17).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Miles within the system of Bunker and Berstis because it would identify the node that has unknown header value.

Regarding claims 16, and 34, Bunker and Berstis and Miles teach all the subject matter as described above. In addition Miles teaches a method/program, wherein the at least one of the procedures further includes identifying an error message in response to the request (col. 23 lines 66-col. 24 lines 17).

Regarding claims 17, and 35, Bunker and Berstis and Miles teach all the subject matter as described above. In addition Bunker and Berstis further discloses the method/program product, wherein the at least one of the procedures includes indicating that the risk assessment scan involves the

intermediate device if the response includes the error message (Bunker 0129 and Berstis (col. 5 lines 25-39).

Allowable Subject Matter

5. Claims 10-14 and 28-32 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Art Unit: 2136

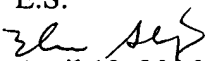
7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867.

The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.


April 13, 2006


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER